

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 25 November 2010 has been entered.

Response to Amendment

2. Applicant's amendment filed 25 November 2010 cancels claims 1-94. Claims 95-101 have been added. Applicant's amendment has been fully considered and entered.

Election/Restrictions

3. Newly submitted claims 98-101 are directed to an invention that is independent or distinct from the invention originally claimed for the following reasons:

Group 1: claims 95-97 associate with previously elected invention (election dated 18 July 2008)

Group 2: claims 98-101 are directed to monitoring hooked functions that are called due to a memory-related action.

4. Since applicant has received an action on the merits for the originally presented invention, this invention has been constructively elected by original presentation for prosecution on the merits. Accordingly, claims 98-101 withdrawn from consideration as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP § 821.03.

Response to Arguments

5. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. Claim 95 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson, U.S. Patent No. 7,689,563, in view of Luke, U.S. Patent No. 6,813,712. Referring to claim 95, Jacobson discloses a policy compliance monitor that provides network user compliance monitoring with network security policy stored in a database by monitoring network activity (Col. 5, lines 36-47), which meets the limitation of a monitoring and capturing sub-system configured to monitor activities relating to communication peripherals and to detect and to act against suspicious or dangerous activity. The database includes encrypted data (Col. 26, lines 15-21), which meets the limitation of an encrypted database storing default security rules including default rules, pre-distribution rules, additionally-acquired user-defined rules, statistics of

acceptable program behavior continuously learned during system operation. The claimed content of the database has not been given patentable weight because the information represents nonfunctional descriptive material that does not impart functionality (MPEP 2106.01). The policy compliance and reporting module monitors and records user and network system activities (Col. 5, lines 53-57), which meets the limitation of wherein accesses to the encrypted database is tracked by the monitoring and capturing sub-system. Jacobson does not disclose monitoring of storage devices. Luke discloses monitoring hard disk activity (Col. 4, lines 15-20), which meets the limitation of monitoring activities relating to storage devices to detect and to act against suspicious or dangerous activity. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the system of Jacobson to monitor hard disk activity because excessive hard drive activity is a symptom of virus infection as taught by Luke (Col. 4, lines 15-20).

9. Claim 96 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson, U.S. Patent No. 7,689,563, in view of Luke, U.S. Patent No. 6,813,712, and further in view of Townsend, U.S. Patent No. 6,374,358. Referring to claim 96, Jacobson does not disclose that the network security policy is generated based upon a questionnaire presented to a user. Townsend discloses generated security policies based upon questionnaires (Col. 3, lines 38-45), which meets the limitation of stores a log of security questions presented to users and replies thereto. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the network security policy of Jacobson to be generated based upon questionnaires in order to determine that the policy is created by appropriate personnel as suggested by Townsend (Col. 3, lines 39-41).

10. Claim 97 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson, U.S. Patent No. 7,689,563, in view of Luke, U.S. Patent No. 6,813,712, and further in view of Lingafelt, U.S. Patent No. 7,013,394. Referring to claim 97, Jacobson does not disclose that the email management system stores email messages of interest. Stolfo discloses storing email messages of interest in a database as signatures (Col. 10, lines 30-33), which meets the limitation of the encrypted database further stores a log of detected suspicious activities. It would have been obvious to one of ordinary skill in the art at the time the invention was made to store email messages of interest in the database of Jacobson in order to provide the ability to detect malicious content in email messages as taught by Lingafelt (Col. 10, lines 30-33).

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432